

Is rodriguezadams.com a scam? TrustSniffer's high-risk assessment:
0/100

rodriguezadams.com

Verdict

0

OUT OF 100

CRITICAL RISK

rodriguezadams.com shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-08-20 by automated analysis. Classification confidence 55%.

What this site appears to be

Password-protected online shop named RodriguezAdams offering a 30% email signup discount, with an email subscription form and a storefront password gate. Contains GDPR/privacy notice and link for store owner login.

Evidence status and limitations

Evidence completeness: UNKNOWN

- The real-world operator identity was not independently verified.
- Module-level completeness metadata is unavailable for this legacy report.

At a glance

The checks that decide most of this verdict.

Malware engines	5 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	4.8 years old Registered history	CLEAR
Web archive	Archived since 2004 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YE2	NOTED

The page as captured

<https://www.rodriquezadams.com/password>



What rodriquezadams.com served when TrustSniffer captured it on 2026-08-20. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2004.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

Fortinet, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

This website is a password-protected Shopify ecommerce storefront branded "RodriguezAdams," presenting visitors with a 30% discount for email subscription while restricting access to the underlying shop; its apparent business model is direct product sales supported by promotional marketing.

Scam/Impersonation Risk

The site presents a relatively ordinary storefront interface, and no conflicting legal identities or brand-impersonation indicators were identified in the supplied page analysis. However, the domain is **blacklisted** by multiple external sources, with corroborated malicious detections, creating a material contradiction that outweighs the benign appearance of the password-gated shop. The site also exposes a password-entry form and collects email subscriptions, while observed browsing generated non-whitelisted external requests and posts; these findings do not establish the precise mechanism of harm but materially increase the risk of sensitive interaction. Historical records do not establish a suspicious repurposing conclusion in the supplied archive assessment, but they do not offset the current external threat detections.

EVIDENCE

- External reputation assessment recorded 5 malicious detections and a confirmed blacklist from two external sources.
- The password page contains a password form and an email-subscription form, as observed in the storefront DOM.
- Browser observation recorded 10 external XHR requests, 8 external posts, 2 non-whitelisted XHR requests, and 4 non-whitelisted posts.
- Archive records show first observation on 2004-04-03, last observation on 2025-01-30, and 22 years tracked.

Regulatory Verification Notes

The available evidence does not independently verify the real-world operator behind RodriguezAdams. The storefront displays a GDPR/privacy statement concerning collection and use of personal information, but the supplied pages do not state a licensing authority, registration number, or other independently checkable regulated-entity credential. That is a disclosure gap rather than standalone proof of fraud; in this case, however, it must be considered alongside the confirmed external blacklist. The domain was registered through Namecheap Inc., and the site uses valid domain-validated TLS, which confirms transport encryption but does not authenticate the operator or establish merchant legitimacy.

EVIDENCE

- Domain registration: 2021-10-30T00:05:20Z; age 4.81 years; expiry 2027-10-30T00:05:20Z; registrar Namecheap Inc.
- Hosting telemetry: served from AS13335, CLOUDFLARENET - Cloudflare, Inc., US.
- TLS telemetry: certificate issuer YE2; validation level DV; valid to 2026-10-03T05:57:32+00:00.
- The storefront privacy notice states that personal information is handled in accordance with European Union regulations, without identifying a licensing authority or registration number.

What to Verify Next

Before any account, credential, or payment interaction, an independent check should establish the merchant's legal identity, physical business details, refund and delivery terms, and the entity responsible for the privacy notice. Any claimed commercial registration or sector-specific authorization should be confirmed directly with the relevant official registry rather than through the website. Contact channels should be validated through an independent route, and the domain should remain subject to enterprise web filtering and malware inspection until the blacklist status is resolved by authoritative review.

EVIDENCE

- The password page provides only a storefront access gate and a store-owner login link, so merchant identity should be obtained from independent documentation.
- The privacy notice provides a regulatory reference but does not, in the supplied content, identify the responsible legal entity.
- The available page analysis records no independently verified licensing authority or registration number.

Summary Verdict

The overall posture is critical, with a high likelihood that sensitive interaction would expose the organization or user to unacceptable security and transaction risk. The website’s polished storefront presentation is insufficient to overcome the converging external threat evidence, and operator legitimacy remains unverified.

Infrastructure Integrity

Cloudflare CDN/WAF protection is present, and the observed address belongs to Cloudflare edge infrastructure rather than an identified origin. This provides a meaningful mitigation against direct origin exposure but is only an infrastructure-control signal and does not validate the website’s content, operator, or reputation.

Closing Assessment

Sensitive interaction should be suspended pending independent confirmation of the merchant and resolution of the external blacklist findings; credentials, payment details, and other personal information should not be submitted in the interim.

Written analysis generated 2026-08-20 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by registration and ownership, analysis engine, behaviour in a sandbox, external reputation.

01 Governance Risk

- The registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.
Registration and ownership rule:KF_WHOIS_PRIVATE

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- The page exchanged network traffic with destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.
External reputation rule:EXT_BLACKLIST_CRITICAL

Identity verification

Status	UNVERIFIED
Identity score	30/100

Identity verification confidence	25%
----------------------------------	-----

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of rodriguezadams.com.

- The request stayed on rodriguezadams.com. It was not redirected to another domain. CLEAR
- Registration is published under NAMECHEAP INC. CLEAR
- DNS for this domain is served by registrar-servers.com, across 2 name servers. NOTED
- The registration is paid up to 2027-10-30. CLEAR
- The earliest public archive of this site is from 2004-04-03. CLEAR
- It is hosted on CLOUDFLARENET, from a server in CA. NOTED

Domain intelligence

Registrar	NAMECHEAP INC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	CA
Server IP	2620:127:f00f:e::
Name servers	PDNS1.REGISTRAR-SERVERS.COM, PDNS2.REGISTRAR-SERVERS.COM
SSL issuer	YE2
SSL expiry	2026-10-03
Domain age	4.81 years (continuous registration)
Domain expiry	2027-10-30
Archive first seen	2004-04-03
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 5 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about rodriguezadams.com at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

